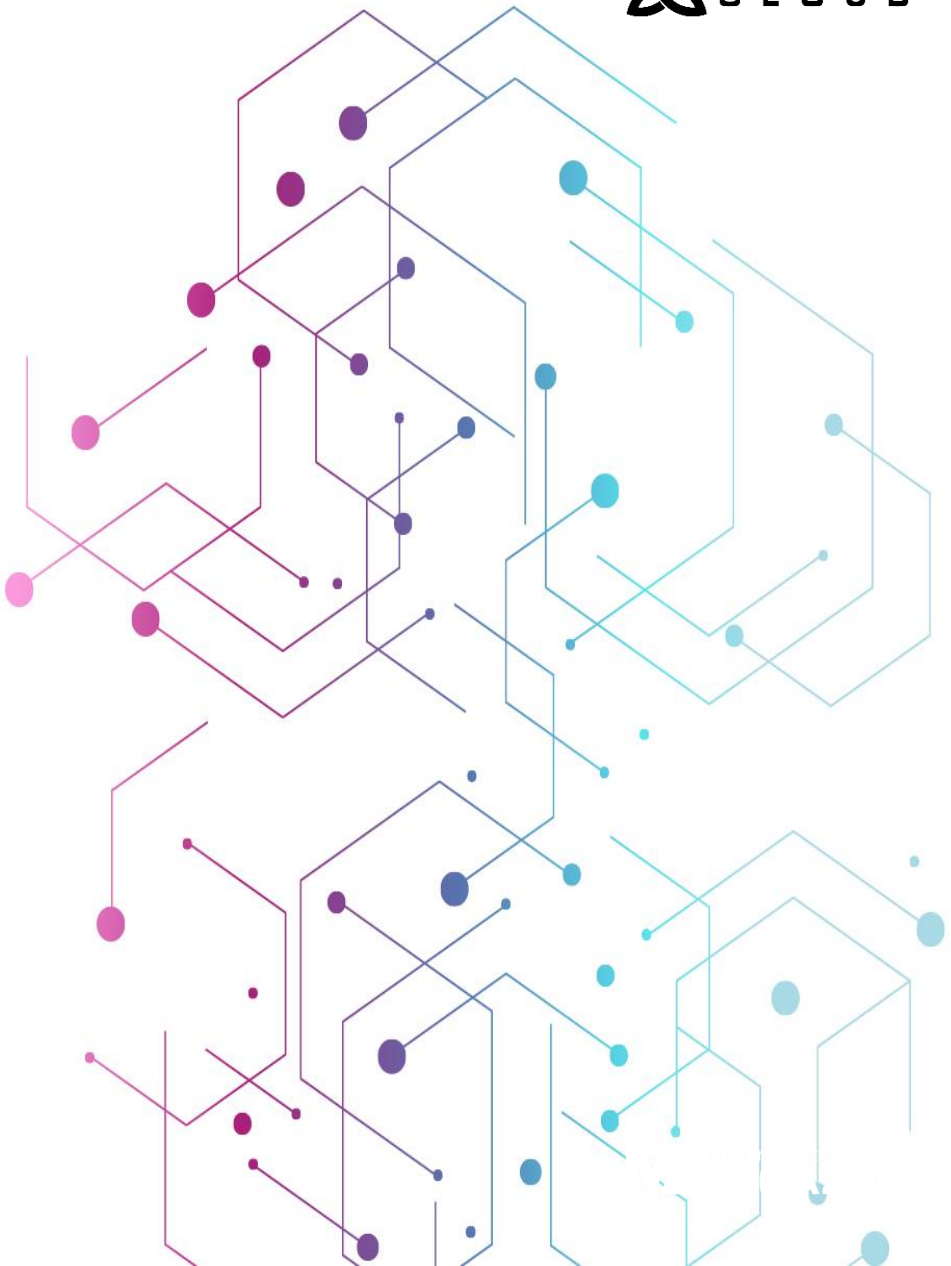
# Elastic Stack 기반 컨테이너 모니터링




**Data Service Center**

**박호동**


2019.09.09

# Summary

Megazone Cloud 소개

Elastic Stack 소개

Elastic Stack 기반 컨테이너 모니터링

- Docker
- Kubernetes
- Use Case

# Megazone Cloud 소개

- 디지털 비즈니스 서비스 경험을 바탕으로 클라우드 사업을 원하는 고객에게 최상의 클라우드 서비스 제공
- 클라우드 컨설팅, 구축, 운영 전문 기업으로 AWS를 비롯한 다양한 클라우드 사업 진행.

amazon web services | Partner Network

PREMIER CONSULTING PARTNER

CHANNEL RESELLER PARTNER

MARKETING & COMMERCE COMPETENCY

AWS GOVERNMENT PARTNER PROGRAM

MANAGED SERVICE PARTNER


2016 AWS '올해의 파트너상' 수상

## Data Service Center

- 클라우드 기반의 데이터 사업 수행
- 빅데이터, DW, Elastic Stack 기반 DataLake, Bigdata System 구축

[주요 사업 실적]

- 웅진 씽크빅 빅데이터 시스템 구축
- S면세점 데이터 레이크 구축
- K카드사 데이터 레이크 구축

## 박호동

- 데이터 엔지니어
- Elastic Cloud 구축
- Elastic Stack 기반 DataLake 구축



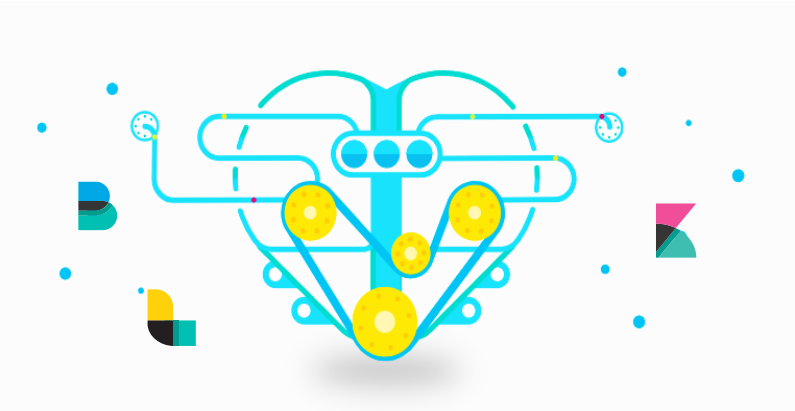


MEGAZONE CLOUD

# Elastic Stack 소개 > Elasticsearch

- 뛰어난 확장성을 제공하는 오픈소스 기반의 Full-text 검색엔진
- 방대한 양의 데이터를 빠르게 저장, 검색, 분석 가능
- 시계열 데이터 분석에 뛰어난 퍼포먼스를 발휘

## The Heart of the Elastic Stack



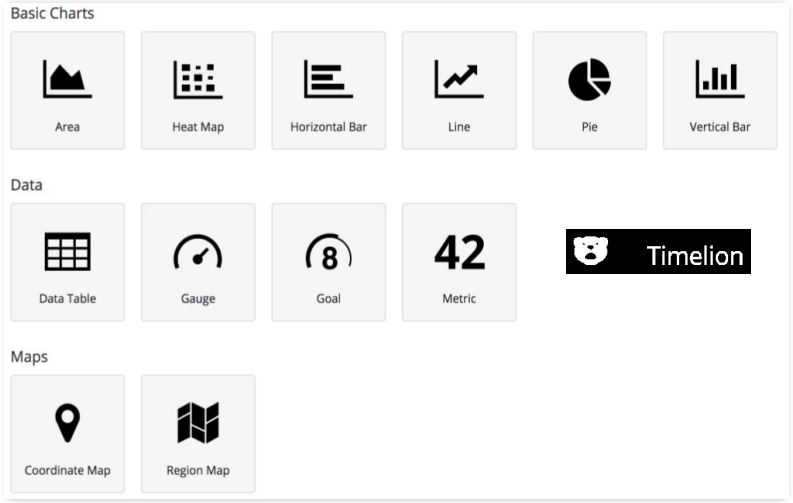
## 기능 및 강점

- **방대한 데이터 조사, 분석, 시각화, 임시 질의 수행**
- Aggregation 기능 지원
- 복잡한 비즈니스 인텔리전스 쿼리를 수행
- 데이터 분석, 추이, 통계, 요약 정보 확인
- 문서를 색인하는 시점부터 검색 가능 대기 시간(약 1초)
- 콘텐츠 볼륨의 수평 분할/확장
- **샤드 분산 배치로 성능/처리량 증가**
- **리블리카 생성으로 고가용성 제공**

# Elastic Stack 소개 > Kibana

- Elasticsearch 와 함께 사용하도록 설계된 오픈소스 분석 및 시각화 플랫폼
- Elasticsearch 쿼리의 변경 사항을 실시간으로 표시하는 동적 대시보드 생성, 공유

## Kibana 지원 분석도구



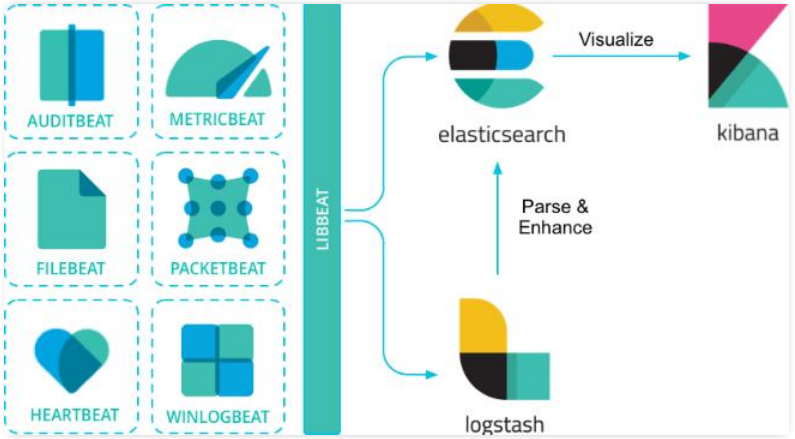

## 기능 및 강점

- **다양한 형태의 데이터 분석도구 제공**
- 수집된 데이터의 관계성 확인
- 시계열 분석을 통해 다양한 그래프 생성
- Kibana에서 제공하는 시각화 도구
  - Basic Charts
  - Data (Metic 등)
  - Maps (위치정보)
- Timelion

# Elastic Stack 소개 > Beats

- Go 언어로 개발된 경량 수집 agent
- 제품별로 특화된 기능이 구분되어 있어 수집하려는 데이터의 성격에 맞는 제품(기능)만 설치 가능

## 경량 수집 agent beats




## 제품별 기능

- Auditbeat : Audit data
- **Filebeat : 로그 등 file data**
- Functionbeat : Cloud data
- Heartbeat : Application health check
- Journalbeat : Systemd journals
- **Metricbeat : Metric data**
- **Packetbeat : Network traffic data**
- Winlogbeat : Windows event logs

# Elastic Stack 강점

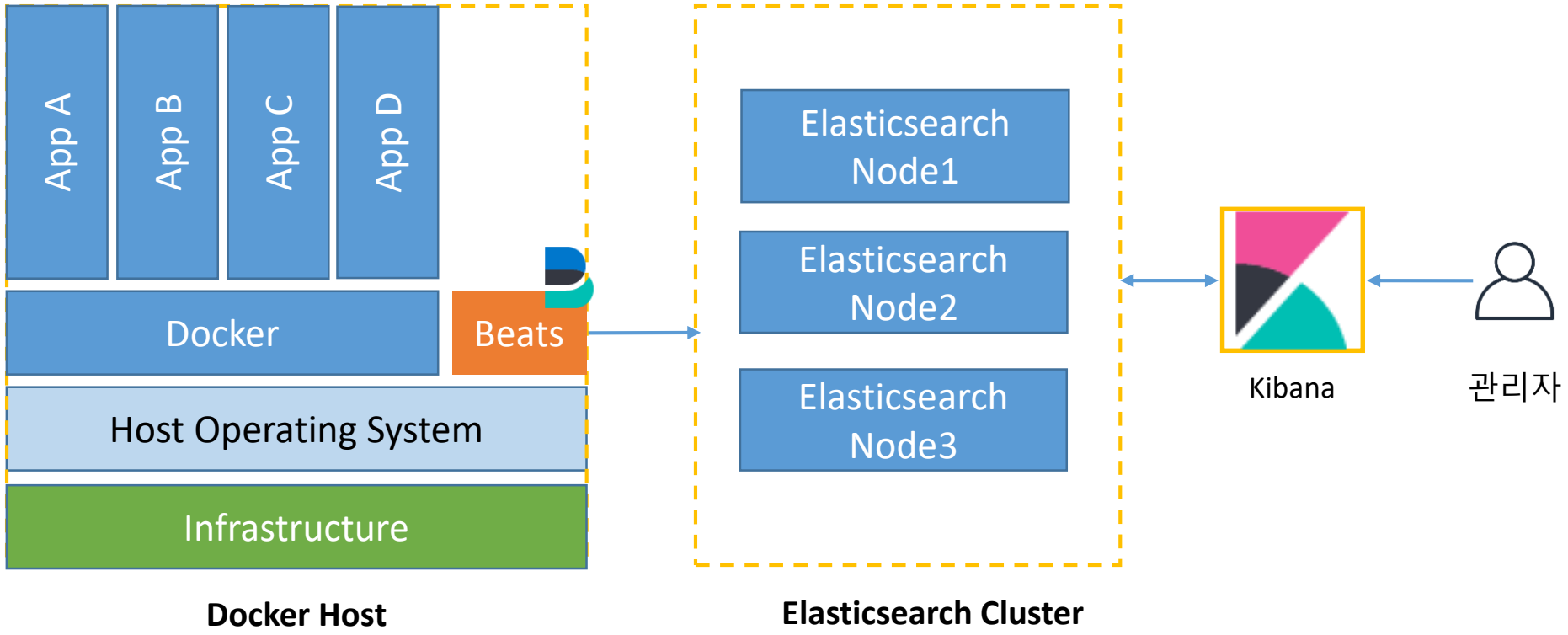
- **강력한 성능의 경량 수집기 Beats**
  - ✓ 다양한 형태의 데이터를 간단한 설정을 통해 수집 가능
  - ✓ 특히 자주 사용되는 데이터 유형은 모듈로 이미 template화 되어 제공

- **실시간 데이터 수집 및 분석**
  - ✓ Elasticsearch는 데이터 적재 시점으로부터 수초 내에 검색 가능

- **데이터 보존**
  - ✓ ILM : 데이터를 생성 주기에 따라 중/장기적으로 보관하기 위한 Index Lifecycle Management 제공
  - ✓ Rollup : (원본 데이터 용량이 큰 경우) 주기적으로 통계 데이터로 변환 후 사이즈가 적은 통계 데이터만 보관 가능

- **Kibana의 다양한 분석 도구 활용**
  - ✓ Discover : 데이터 분석 전략 수립 및 원본 데이터 확인
  - ✓ 시각화, 대시보드 : 실시간 데이터 분석
  - ✓ Canvas : 보고서 생성

# Docker Monitoring Simple Architecture







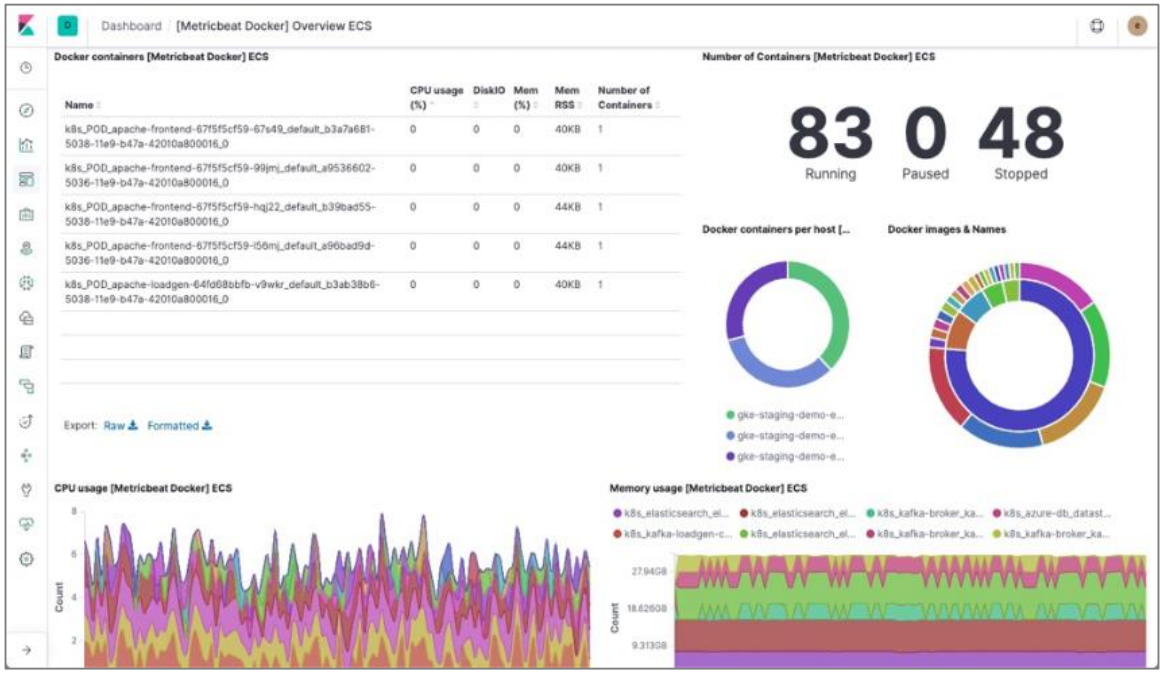

MEGAZONE CLOUD

# Docker Metric Monitoring > Metricbeat Docker 모듈 활용

- **모듈이란?**
  - ✓ 자주 사용되는 데이터 유형을 수집하기 위한 설정을 개발사에서 미리 template화 하여 제공하는 기능
  - ✓ 모듈에 따라 설정 뿐 아니라 Kibana Sample Dashboard가 제공되는 경우도 있음

- **수집방식**
  - ✓ Fulling 방식
  - ✓ 일정 주기마다 Docker API 호출

- **사용방법**
  - ✓ Metricbeat 설치
  - ✓ Docker 모듈 활성화
  - ✓ Metricbeat.yml 파일 수정
  - ✓ Metricbeat setup
  - ✓ Metricbeat 실행







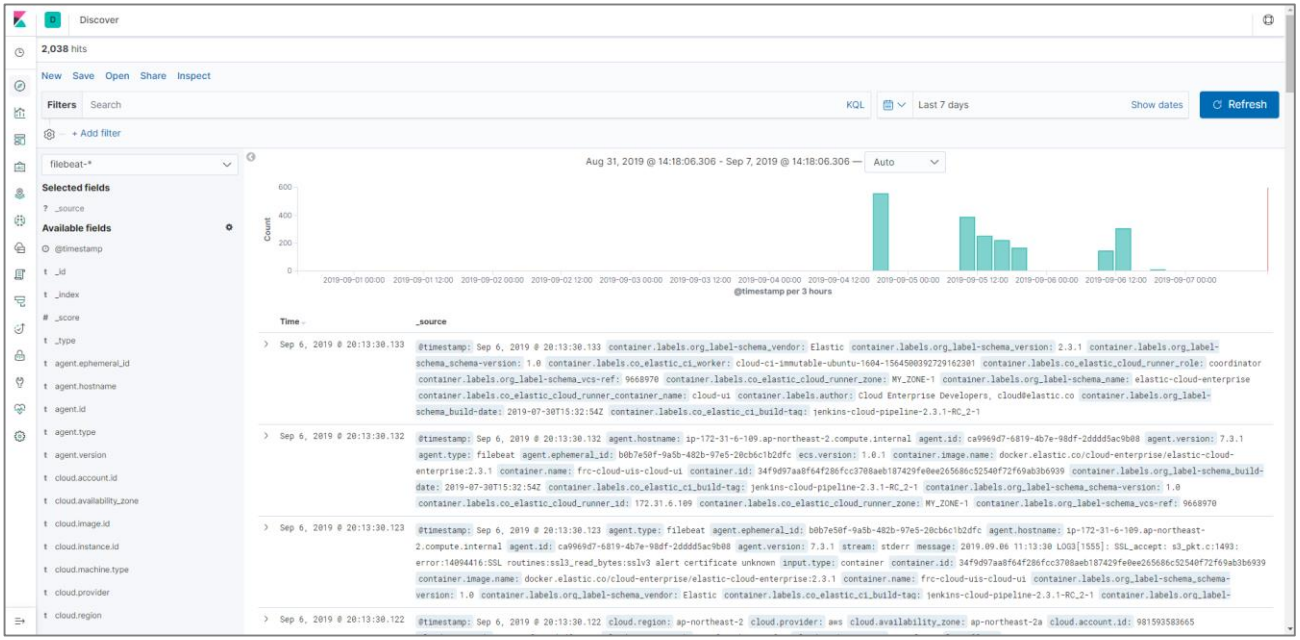

MEGAZONE CLOUD

# Docker Log Monitoring > Filebeat 활용

- **Docker의 로그**
  - ✓ 엔진 로그 : 일종의 공통 로그 (컨테이너 생성시부터 컨테이너가 정상적으로 로드될 때 까지의 정보를 표시)
  - ✓ 컨테이너 로그 : 컨테이너에서 실행되는 Application에서 생성하는 로그

- **사용방법**
  - ✓ Filebeat 설치
  - ✓ filebeat.yml 파일 수정
  - ✓ Filebeat setup
  - ✓ filebeat.yml 소유자 변경
  - ✓ Filebeat 실행

- **주의사항**
  - ✓ root 권한으로 실행



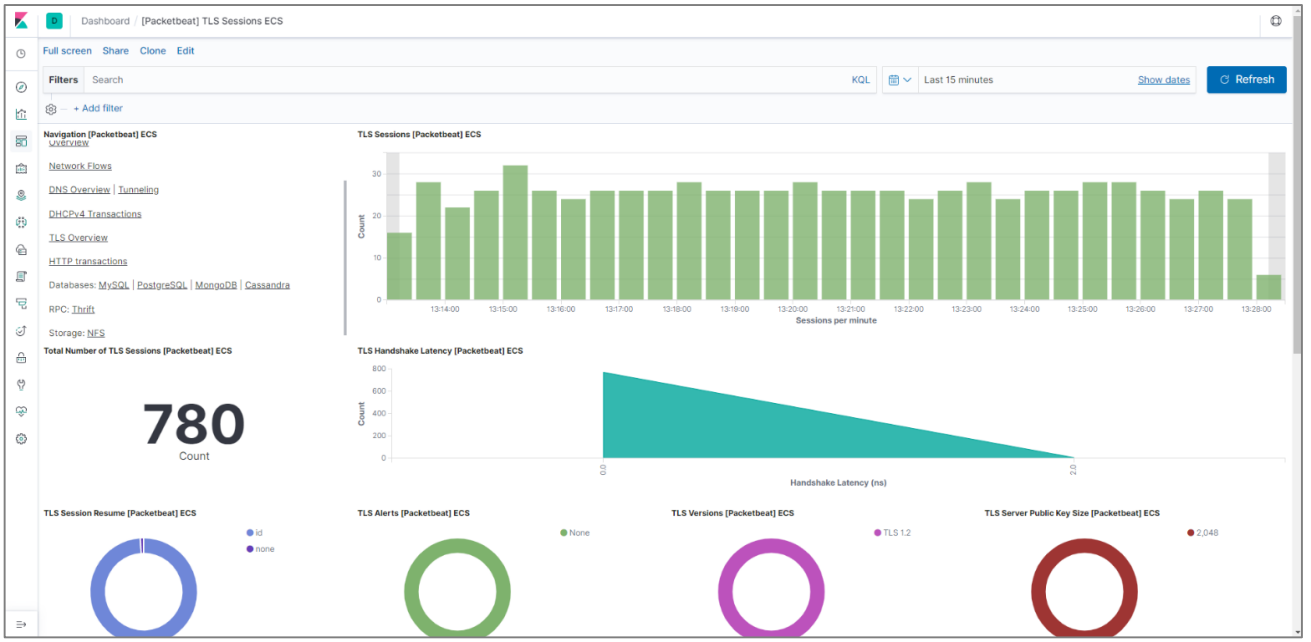





MEGAZONE CLOUD

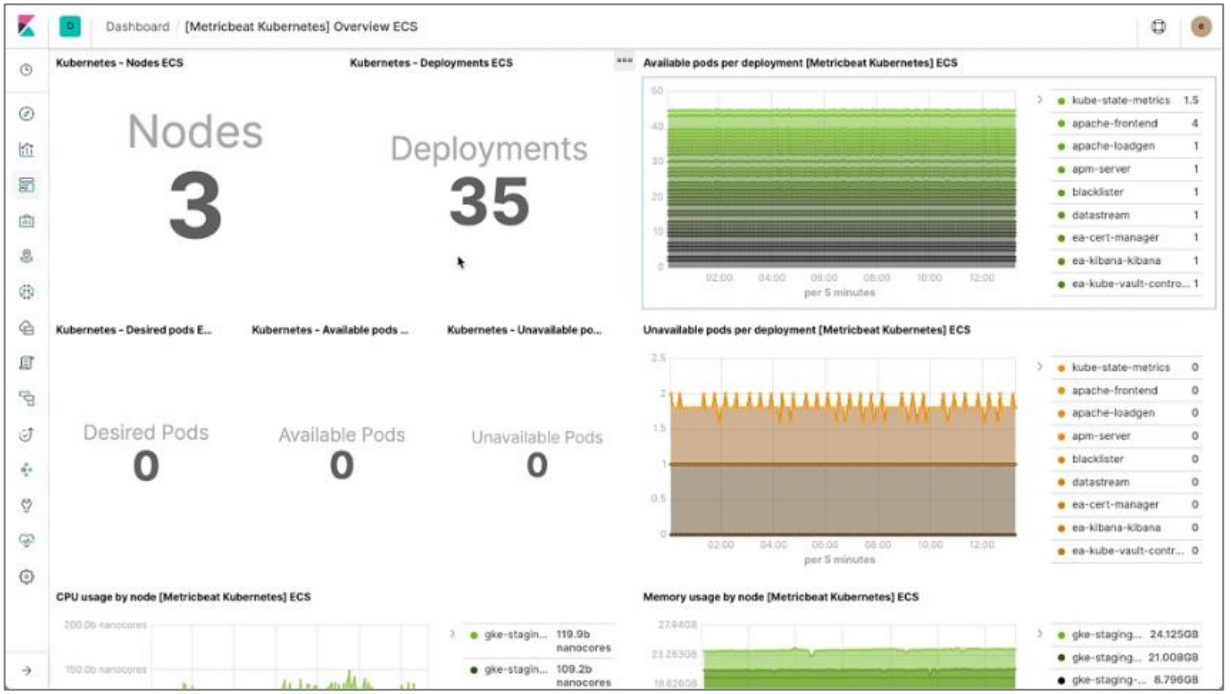
# Docker Network Traffic Monitoring > Packetbeat 활용

- **Network Traffic : Packetbeat이 설치된 서버에서 인식되는 Network 장비(NIC)에서 다음에 해당하는 정보들을 수집 가능**
  - ICMP (v4 and v6), DHCP (v4)
  - AMQP 0.9.1, Redis, Memcache
  - DNS
  - HTTP, TLS
  - Cassandra, MongoDB
  - Mysql, PostgreSQL
  - Thrift-RPC, NFS
- **사용방법**
  - Packetbeat 설치
  - packetbeat.yml 파일 수정
  - Packetbeat setup
  - packetbeat.yml 소유자 변경
  - Packetbeat 실행
- **주의사항**
  - root 권한으로 실행



# Kubernetes Metric Monitoring > Metricbeat K8s 모듈 활용

- **사용방법**
  - ✓ Metricbeat 설치
  - ✓ Kubernetes 모듈 활성화
  - ✓ metricbeat.yml 파일 수정
  - ✓ Metricbeat setup
  - ✓ Metricbeat 실행








MEGAZONE CLOUD

# Kubernetes Metric Monitoring > Metricbeat K8s 모듈 데이터셋

| | |
|---|---|
| API Server | State Container |
| Container | State deployment |
| Controller manager | State Node |
| event | State Pod |
| Node | State replicaset |
| Pod | State statefulset |
| Proxy | System |
| Scheduler | Volume |

# Kubernetes Log Monitoring : Filebeat 활용

- **사용방법**
  - ✓ Filebeat 설치
  - ✓ filebeat.yml 파일 수정
  - ✓ Filebeat setup
  - ✓ filebeat-kubernetes.yml 다운로드
  - ✓ filebeat-kubernetes.yml 파일 수정
  - ✓ kubectl을 사용하여 Filebeat 실행

- **주의사항**
  - ✓ Filebeat 설치 시 패키지 매니저를 통한 설치 필요
  - ✓ filebeat-kubernetes.yml 설정상 Filebeat 이미지가 6.3.2 버전 기준 이미지

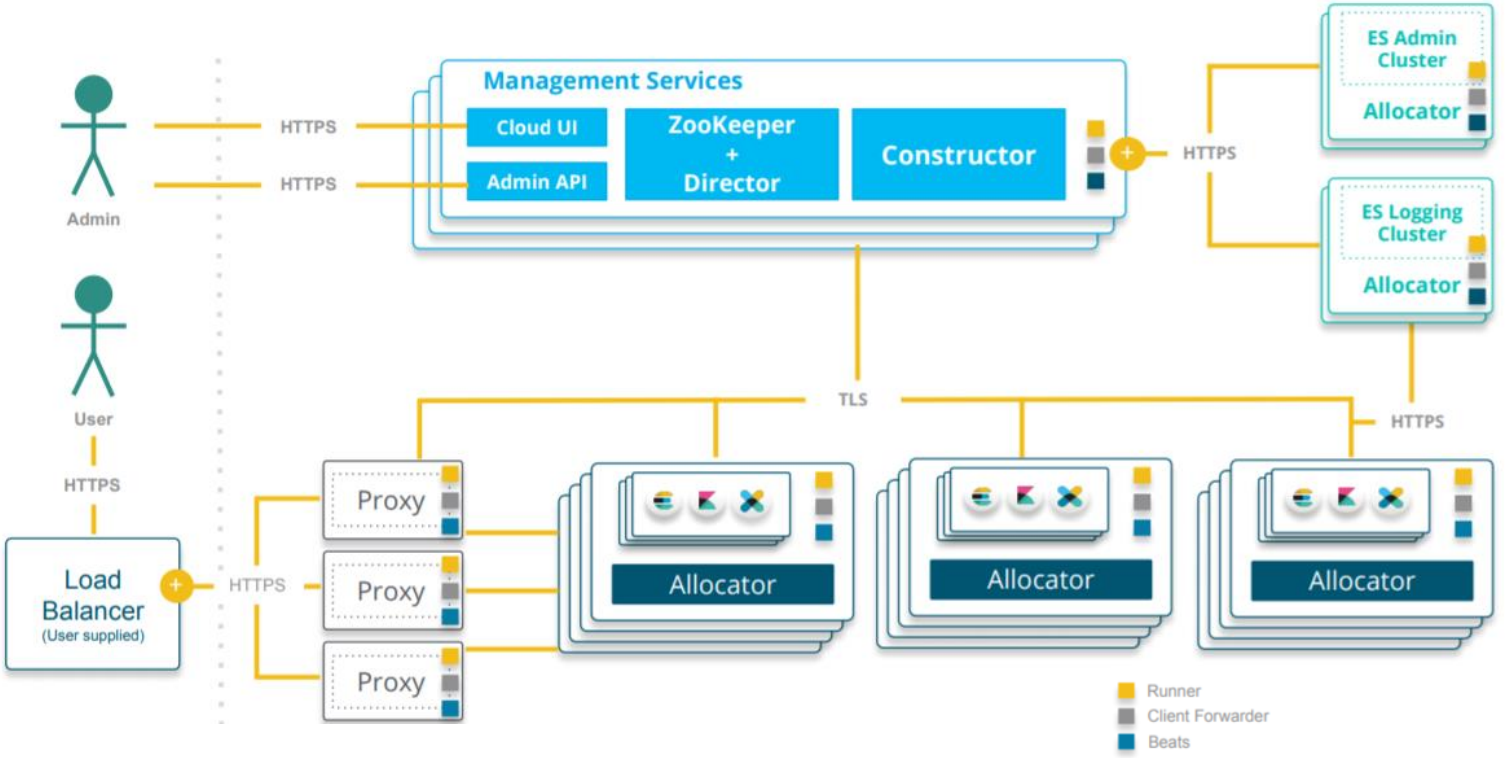
# More Information > Elastic Stack 추가 기능 소개

- **Watcher**
  - ✓ Cron 형식 또는 단순 스케줄러 제공
  - ✓ 조회결과를 조건에 따라 실행여부 결정
  - ✓ 활성화 된 Job의 실행결과를 히스토리로 제공
  - ✓ Email, Slack, Jira 등 다양한 외부 Notification 기능과 연동 가능

- **Machine Learning**
  - ✓ 시계열 데이터의 이상감지(anomaly detection)에 뛰어난 데이터 분석 알고리즘을 제공
  - ✓ 과거 데이터를 학습하여 새로 입력된 데이터가 정상 범주에 속하는 데이터인지 판단
  - ✓ 새로 추가되는 데이터를 재학습하여 계속해서 모델링을 보완
  - ✓ Watcher와 연계하여 이상감지시 필요한 방식으로 Notification 가능

# Elastic Cloud Enterprise 소개

- Cloud, 베어메탈 등 어느 장비에나 Elastic Cloud를 구현할 수 있도록 개발된 Docker 기반 설치형 제품
- 중앙 집중식 클러스터 관리를 위한 Admin UI 제공
- Allocator, Director, Proxy 등의 내부 기능을 Docker 컨테이너로 구성








MEGAZONE CLOUD

# Use Case 1. 사내 데이터 분석용 Docker 호스트 모니터링

- **문제인식**
  - ✓ 데이터는 Elasticsearch 및 Hadoop으로 지속적으로 적재중
  - ✓ 분석가들이 사용하기 위한 각종 분석도구들이 Docker로 제공됨
  - ✓ 분석가들의 컨테이너 생성 및 삭제에 대한 통제는 잘 되고있지 않았음
  - ✓ on-premise 환경으로 서버 하나를 다수의 Application이 점유할 수 밖에 없는 상황
  - ✓ 시스템 관리자는 현재 어떤 컨테이너가 리소스를 많이 사용하고 있는지, 해당 컨테이너에서 실행중인 Application이 무엇인지 모니터링 할 수 있기를 희망함
  - ✓ 특정 호스트에 컨테이너가 집중 배치된 경우 인지할 수 있기를 희망함

- **문제해결**
  - Metricbeat Docker, System 모듈을 사용하여 모든 분석용 Docker Host의 지표를 Elasticsearch로 수집
  - 수집된 지표를 Kibana에서 확인하기 위해 대시보드 커스터마이징

# Use Case 2. Docker 기반 서비스 모니터링

- **문제인식**
  - ✓ 사내에 구성된 Docker 기반 서비스(ECE)의 운영을 이원화해서 관리 (인프라/Application)
  - ✓ 전체 시스템은 문제가 없고 특정 서비스에서 정상적인 요청에도 Error Code가 응답되는 경우가 발생
  - ✓ 알람 서비스는 인프라 운영팀에서 제공되었는데, 인프라 레벨에서는 서비스 이상여부 검출이 어려움

- **문제해결**
  - ✓ Metricbeat Docker, System 모듈을 사용하여 필요한 모든 Docker Host의 지표를 Elasticsearch로 수집
  - ✓ Docker Host에 설치되어 있는 Metricbeat에 Elasticsearch, Kibana 모듈을 추가 적용
  - ✓ 문제 발생시 원인 파악을 위해 컨테이너에서 실행중인 서비스 로그까지 모두 수집
  - ✓ 주기적으로 관리가 필요한 클러스터 상태를 체크하여 이상이 있는 경우 Slack으로 알림 메시지 전송

# 기대효과

- **간편한 컨테이너 모니터링 시스템 구축**
  - ✓ Kibana의 다양한 분석용 도구들을 활용하면 나만의 대시보드 구성 가능
  - ✓ 직관적인 대시보드 구성에 성공한다면 시스템에 문제가 발생했을 때 보다 신속하게 확인 가능
  - ✓ 정기적인 보고서가 필요하다면 리포팅 대시보드 또는 캔버스 구성 가능

- **컨테이너 관리 시스템 자동화 -> 삶의 질 향상**
  - ✓ Elasticsearch 모든 기능은 RESTFul API로 제공 -> json 파서만 있다면 어느 언어라도 연동 가능
  - ✓ 빈번하게 발생하는 비슷한 패턴의 시스템 이슈가 있다면 이는 자동화 대상
  - ✓ 단, 관리자가 혼자라면 자동화까지는 힘들 수도 있음

# THANK YOU



http://www.cloud.hosting.kr | http://www.mz.co.kr
46, Nonhyeon-ro 85-gil, Gangnam-gu, Seoul, Korea | T. 1644-2243